State of Michigan Evaluation of the Internal Control Structure (ICS) In Effect During the Two-year Period Ended September 30, 20

Description of Departmental Activity:	- Worksheet for Evaluating "General Controls" over Automated Information Systems -
Information System Evaluated:	

NOTE: Due to the formation of the Department of Information Technology (DIT), many IT related responsibilities that were formerly assumed by Agency/Department Management has shifted to DIT Management. <u>DIT Management is responsible for the State of Michigan's entire General Control environment</u>. <u>In addition, DIT Management is the business process/application owner for DIT applications and holds responsibility for managing its' applications and their application environment.</u>

GENERAL CONTROLS

[General controls provide the business and IT functions with a set of encompassing controls that are shared by several business or information system functional units, or support underlying functions that one or more applications rely on. General controls commonly include controls over data processing center operations, system software (not application software), databases, acquisition and maintenance, access security (both physical and logical), application systems development maintenance, and overall IT Department administration. These controls apply to all systems-mainframe, mini-computer, and end-user computing environments.]

physical and logical), applic	ation systems development maintenance	e, and overall IT Department administration. The	ese controls apply to a	ll sys	tems-	mainfra	ame, m	ini-c	ompute	er, and end	d-user computing environments.]
achievement of the busines	y and tactics, and concerns the identificates objectives. Furthermore, the realization and for different perspectives. Finally, a pro-	tion of the way IT can best contribute to the n of the strategic vision needs to be planned, oper organization as well as technological	Assessment of Actual Internal Controls						Controls -		
				E	xister	тсе**:	Perfo	rman	nce/Effe	ctiveness:	
IT PROCESS:	POTENTIAL/LIKELY RISKS:	OBJECTIVE (To address risks):	Agency, Division/Office, and Staff (DIT) responsible for IT process and related internal controls: (1)	Documented	Not Documented	Not Sure or Not Applicable	Excellent	Excellent Very Good Satisfactory Ineffective/ Inefficient		Not Sure or Not Applicable	Description/Comments (Explanation of written procedures/practices: control system strengths & weaknesses):
Define a strate via IT											
Define a strategic IT plan CobiT Reference: PO 1.0	Failure to adequately balance information technology opportunities to IT department requirements, and ensure the IT plans further accomplishment.	Is there a periodic strategic planning process providing long-term plans, which are translated into operational plans, setting clear and concrete short-term goals? (Refer to "Control Objectives" 1.1 - 1.6 to									
CODIT Reference. FO 1.0		determine whether the objective has been met									
Define	Failure to appropriately organize	Has a business information model been									

	T							
information	information systems.	created & maintained; are appropriate						
architecture		systems defined to optimize the use of this	·					
		information?						
CobiT Reference: PO 2.0		(Defer to "Control Chicotives" 2.1 - 2.4 to	•					
Codit Reference. FU 2.0		(Refer to "Control Objectives" 2.1 - 2.4 to determine whether the objective has been						
		met)						
	+	+		+ + +	+++		+ +	
Determine	Failure to utilize available and	Are technological infrastructure strategies		+ + +	-			
		developed and maintained?						
_		·						
CobiT Reference: PO 3.0		(Refer to "Control Objectives" 3.1 - 3.5 to						
		determine whether the objective has been						
		met)		 	-			
Define IT organization	Inability to satisfactorily deliver IT	Is a suitable number of skilled staff employed			+	_		
and relationships	services.	and are their roles & responsibilities defined &						
and relationings	SCI VICES.	communicated?	•					
CobiT Reference: PO 4.0								
		(Refer to "Control Objectives" 4.1 - 4.15 to						
		determine whether the objective has been						
		met)						
<u> </u>	<u> </u>							
Manage IT		Are periodic investment & operational budgets						
Investment	disbursements of financial resources.	established and approved by the department?						
CobiT Reference: PO 5.0		(Refer to "Control Objectives" 5.1 - 5.3 to						
CODIT REICIENCE. FO J.V		determine whether the objective has been	•					
		met)						
	+	+	·		+++		+ +	
Communicate	Lack of user	Are policies established & communicated to		+ + +			1 1	
management aims &	awareness/understanding of	users? Has there been an establishment of						
direction	management objectives.	standards, which translate strategic options						
	_	into practical & understandable rules for						
		users?						
CobiT Reference: PO 6.0		(Refer to "Control Objectives" 6.1 - 6.11 to	•					
		determine whether the objective has been	•					
	+	met)		+++	+	_	+ +	
Manage Personnel	Inability to maximize staff	Are sound personnel management techniques		++++	+			
Ivianago i crooo.		used?	•					
	Contributions to 11 processes.	usea:						
CobiT Reference: PO 7.0		(Refer to "Control Objectives" 7.1 - 7.7 to						
		determine whether the objective has been						
		met)						
Ensure compliance with	Failure to satisfy legal, regulatory or	Has the impact of external requirements been						
external requirements	contractual obligations.	Identified & analyzed; has appropriate action						
		been taken to comply with them?						

CobiT Reference: PO 8.0		(Refer to "Control Objectives" 8.1 - 8.6 to determine whether the objective has been met)					
Assess Risks	Inability to achieve IT objectives; inability to respond to threats to	Has management* identified risks to IT; completed an impact analysis; implemented					
CobiT Reference: PO 9.0	provision of IT services.	cost-effective measures to mitigate risk? (Refer to "Control Objectives" 9.1 - 9.6 to determine whether the objective has been met)					
Manage Projects CobiT Reference: PO 10.0	Failure to set priorities; inability to meet deadlines or stay within budget.	Are projects identified & prioritized in accordance with an operational plan; are sound management techniques adopted for each project? (Refer to "Control Objectives" 10.1 - 10.13 to determine whether the objective has been met)					
Manage Quality	Failure to meet customer	Have quality management standards and					
CobiT Reference: PO 11.0	requirements.	systems been implemented, and maintained as part of the organizational plan? (Refer to "Control Objectives" 11.1 - 11.19 to determine whether the objective has been met)					

⁽¹⁾ Identify the activity (i.e., specific divisions, application owners/user agencies, vendor/contractor, etc.) responsible for IT process and associated internal controls. *Your Department/Agency Management
**When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements

ntegrated into the business p	solutions need to be identified, develo	ped or acquired, as well as implemented and naintenance of existing systems are covered by stems.	by				l Controls -						
					Existence**:			forma	ance/E	ffectivene	ness:		
OBJECTIVE:	POTENTIAL/LIKELY RISKS:	OPTIMAL INTERNAL CONTROLS (To address risks):	Agency, Division/Office, and Staff (DIT) responsible for IT process and related internal controls: (1)	Documented	Not Documented	Not Sure or Not Applicable	Excellent	Very Good	Satisfactory Ineffective/	Inefficient Not Sure or Not Applicable	Description/Comments (Explanation of written procedures/practices: control system strengths & weaknesses):		

11 (6 4 4 1	Te no contract of the	1		1 1	 1	
Identify automated solutions	Failure to identify best approach to satisfy user requirements.	Has a clear analysis of alternative resolutions been completed, considering user requirements?				
CobiT Reference: Al 1.0		(Refer to "Control Objectives" 1.1 - 1.18 to determine whether the objective has been met)				
Acquire & maintain application software CobiT Reference: Al 2.0	that effectively support departmental	Has management* adopted a methodology that provides for distinct developmental phases; foresees clear phases & deliverables for package acquisitions? (Refer to "Control Objectives" 2.1 - 2.17 to determine whether the objective has been met)				
2 1 0						
Acquire & maintain technology architecture CobiT Reference: Al 3.0	Inability to provide proper platforms for supporting business applications.	Does management* assess hardware & software performance; provisions for preventive hardware maintenance; installation, security & control of system software? (Refer to "Control Objectives" 3.1 - 3.6 to				
		determine whether the objective has been met)				
Develop & maintain IT procedures CobiT Reference: Al 4.0	Inability to ensure proper use of applications & installed technology solutions.	Does management* have a structured methodology for developing user and operational procedure manuals, service requirements, training materials, etc? (Refer to "Control Objectives" 4.1 - 4.4 to determine whether the objective has been met)				
Install & accredit systems	Failure to verify and confirm that a solution addresses its intended purpose.	Has a well-formalized installation, migration, conversion and acceptance plan been Implemented?				
CobiT Reference: Al 5.0		(Refer to "Control Objectives" 5.1 - 5.11 to determine whether the objective has been met)				
Observes	- U test standing	- 41				
Manage Changes CobiT Reference: Al 6.0		Does management* have a management system that provides for analysis, implementation and follow-up of all changes (requested or made) to existing IT infrastructure? (Refer to "Control Objectives" 6.1 - 6.7 to determine whether the objective has been met)				
		,				
				l		

(1) Identify the activity (i.e., specific divisions, application owners/user agencies, vendor/contractor, etc.) responsible for IT process and associated internal controls. *Your Department/Agency Management
**When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements

security and continuity aspeset up.	vith the actual delivery of required service	s, which range from traditional operations over s, the necessary support processes must be stems, often classified under application		Ass	essm	ent	of A	Actu	Controls -			
				E	xister	ce**:	Per	form	anc	e/Effe	ctiveness:	
OBJECTIVE:	POTENTIAL/LIKELY RISKS:	OPTIMAL INTERNAL CONTROLS (To address risks):	Agency, Division/Office, and Staff (DIT) responsible for IT process and related internal controls: (1)	Documented	Not Documented	Not Sure or Not Applicable	Excellent	Very Good	Satisfactory	Ineffective/ Inefficient	Not Sure or Not Applicable	Description/Comments (Explanation of written procedures/practices: control system strengths & weaknesses):
Define service level CobiT Reference: DS 1.0	Inadequate understanding of necessary level of service.	Has management* established service level agreements (both vendors and intradepartmental) that formalize performance criteria against which quantity and quality of service is measured? (Refer to "Control Objectives" 1.1 - 1.7 to determine whether the objective has been met)										
Manage third-party services	Failure to ensure third parties' responsibilities & roles are clearly defined, adhered to, and satisfy specified requirements.	Have measures to review/monitor existing contracts and procedures for their effectiveness and compliance with department policies been implemented?										
CobiT Reference: DS 2.0		(Refer to "Control Objectives" 2.1 - 2.8 to determine whether the objective has been met)										
Manage performance and capacity CobiT Reference: DS 3.0		Have capacity and performance management controls that collect data & report on workload management, application size, resource & demand management been implemented? (Refer to "Control Objectives" 3.1 - 3.9 to determine whether the objective has been met)										

Ensure continuous service	Required customer services are not available.	Does a tested, operational IT continuity plan exist and is it aligned with the overall business plan & related requirements?						
CobiT Reference: DS 4.0		(Refer to "Control Objectives" 4.1 - 4.12 to determine whether the objective has been met)						
Ensure systems security CobiT Reference: DS 5.0	Unauthorized usage, disclosure, modification, damage or loss of data.	Have logical access controls, which restrict access to systems, data & programs to authorized users only, been implemented? (Refer to "Control Objectives" 5.1 - 5.21 to						
Oddir Holorollos. 20 cls		determine whether the objective has been met)						
Identify & attribute/ allocate costs	Unaware of costs attributable to IT related services.	Does the cost accounting system ensure costs are recorded, calculated, & allocated to the required level of detail?						
CobiT Reference: DS 6.0		(Refer to "Control Objectives" 6.1 - 6.3 to determine whether the objective has been met)						
Educate & train Users	Failure to recognize technological risks and responsibilities; failure to use technology effectively.	Has a comprehensive training/development plan been implemented?						
CobiT Reference: DS 7.0	-	(Refer to "Control Objectives" 7.1 - 7.3 to determine whether the objective has been met)						
Assist & advise IT customers	User inability to adequately deal with IT related problems.	Does the help desk facility provide first-line support activities?						
CobiT Reference: DS 8.0		(Refer to "Control Objectives" 8.1 - 8.5 to determine whether the objective has been met)						
Manage the Configuration	all IT components; inability to provide	Have controls been implemented to identify & record all IT assets and their physical location? Is there a periodic verification						
CobiT Reference: DS 9.0	a sound basis for change management.	program to confirm existence of recorded assets? (Refer to "Control Objectives" 9.1 - 9.6 to determine whether the objective has been met)						
		1						

Manage problems & incidents	No resolution to problems or incidents unable to identify their cause in order; to prevent recurrence.	Has management* implemented a problem management system to record progress of all incident resolutions?					
CobiT Reference: DS 10.0		(Refer to "Control Objectives" 10.1 - 10.3 to determine whether the objective has been met)					
Manage Data	Incomplete, inaccurate or invalid data during input, update & storage.	Has management* implemented effective application & general controls over IT operations?					
CobiT Reference: DS 11.0		(Refer to "Control Objectives" 11.17, 11.18, 11.27-11.29, to determine whether the objective has been met)					
Manage Facilities	Unsuitable physical surroundings, does not protect IT equipment or personnel against man-made or natural hazards.	Have appropriate environmental & physical controls been installed and are these controls regularly reviewed for proper functionality?					
CobiT Reference: DS 12.0		(Refer to "Control Objectives" 12.1 - 12.6 to determine whether the objective has been met)					
Manage Operations	Failure to adequately perform orderly, periodic, critical IT support functions.	Is an operations schedule of recorded/cleared support activities maintained?					
CobiT Reference: DS 13.0		(Refer to "Control Objectives" 13.1 - 13.7 to determine whether the objective has been met)					

⁽¹⁾ Identify the activity (i.e., specific divisions, application owners/user agencies, vendor/contractor, etc.) responsible for IT process and associated internal controls. *Your Department/Agency Management
**When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements

IT MONITORING (M) All IT processes need to be re This domain thus addresses assurance provided by intern	Assessment of Actual Internal Controls - ents.							ontrols -				
dodurance provided by intern	al and external addit of obtained from an	terrative sources.	Existence**:						nanc	:e/Effe	ctiveness:	
OBJECTIVE:	POTENTIAL/LIKELY RISKS:	OPTIMAL INTERNAL CONTROLS (To address risks):	Agency, Division/Office, and Staff (DIT) responsible for IT process and related internal controls: (1)	Documented	Not Documented	Not Sure or Not Applicable	Excellent	Very Good	Satisfactory	Ineffective/ Inefficient	Not Sure or Not Applicable	Description/Comments (Explanation of written procedures/practices: control system strengths & weaknesses):
	objectives.	Have relevant management reporting & performance indicators been defined? Are services to be delivered measured against these performance indicators and support systems implemented as necessary? Do management reports provide for review of the organization's progress toward identified goals? (Refer to "Control Objectives" 1.1 - 1.4 to determine whether the objective has been met)										
	security & internal control functionality.	Is management* committed to monitoring & assessing the effectiveness of internal controls and is there periodic reporting on the control structure? (Refer to "Control Objectives" 2.1 - 2.4 to determine whether the objective has been met)										
Obtain independent assurance CobiT Reference: M 3.0	within IT organization or among customer and third-party providers.	Are periodic independent assurance reviews conducted? (Refer to "Control Objectives" 3.1 - 3.8 to determine whether the objective has been met)										

	<u> </u>	I	T						
Provide for	Failure to increase confidence levels	Are periodic independent audits conducted?							
independent audit	in economy, efficiency, effectiveness								
	of IT internal control and security								
	environment; failure to benefit from								
CobiT Reference: M 4.0	best practice advice.	(Refer to "Control Objectives" 4.1 - 4.8 to							
Cobit Reference. W 4.0	· ·	determine whether the objective has been							
		met)							
General Controls - Ov	verall Conclusion/Control System	m Strengths and Weaknesses							·
(1) Identify the activity (i.e.,	, specific divisions, application owners/us	er agencies, vendor/contractor, etc.) responsible	e for IT process and ass	sociate	ed inte	rnal co	ontrols		
*Your Department/Agency		, , ,	·						
	pplicable documentation and/or flowchar	ts for your future needs/requirements							
μ,	P.P	··· • • • · · · · · · · · · · · · · · ·							
Landie dans data	d all a constitues Blates and October	A A M. Marta A. Carrata H. Carratta .	O - (4"		c			
i certify that this eva		ol Activities in Automated Information							
	, in effect	during the two-year period ended 9/3	60/ has been co	ondu	cted i	in a r	easo	nabl	le and prudent manner, and I concur
with the conclusions	s documented above as a result	t of this evaluation.							
Activity Level Ma	anager Signature	Date							